diversiCOM®
Melrose Telephone Company
Mainstreet Communications LLC
Wisper High Speed Internet

PO Box 100
Melrose, MN 56352-0100

Phone: 320-256-7471
Toll Free: 800-554-0185
Fax: 320-256-7555
www.meltel.com

2-10-2009

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

RE: CPNI Annual Filing – EB Docket No. 06-36

Dear Ms. Dortch:

Please find attached is the "Annual CPNI 2007" filing. This filing is being done for the companies named on the attached form. We are following the CPNI rules for all companies, at this time only two (2) companies have Form 499 Filer ID as the third (1) company is high speed wireless company not providing voice but are following all of the CPNI guidelines as the rest of our telecommunications companies.

Any questions feel free to give me a call at 320.256.0205.

Carol M Bertram

Carol Bertram
Director of Industry Relations
CPNI Compliance Officer

encl.

cc: FCC-Enforcement Bureau, Telecommunications Consumers Division
Best Copy and Printing, Inc.-FCC@BCPIWEB.COM

diversiCOM®
Melrose Telephone Company
Mainstreet Communications LLC
Wisper High Speed Internet

PO Box 100
Melrose, MN 56352-0100

Phone: 320-256-7471
Toll Free: 800-554-0185
Fax: 320-256-7555
www.meltel.com

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008
Date filed: 2-10-2009

Name of company covered by this certification diversiCOM: Melrose Telephone Company, Mainstreet Communications, LLC and Wisper Wireless Solutions, LLC

Form 499 Filer ID: 807780,820372

Name of signatory: Carol Bertram

Title of signatory: Director of Industry Relations

I, Carol Bertram certify that I am an officer of the companies named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company currently has no information with respect to the processes pretexters are using to attempt to access CPNI. At this time, we have not encountered known pretexting. Our protective measures against pretexters are outlined in the accompanying statement of operating procedures.

Signed:

Carol M Bertram

Attachment: Accompanying Statement of Operating Procedures

Per the FCC CPNI rules [47 CFR §64.2009(e)] and as referenced in the attached signed certification, (Insert Company Name), herein referenced as the Company hereby certifies that the Company [and its affiliates] is in compliance with the FCC CPNI rules and has outlined some of the important operating procedures below in order to ensure the Company's compliance in the protection of CPNI:

1. CPNI manual has been updated in order to account for all FCC CPNI rules, including the recent revisions, and has been adopted by our Company's board
2. CPNI Compliance officer has been designated to oversee all CPNI duties, training, and activity
    - Established an outbound marketing supervisory review process for the use of CPNI
    - Records are maintained for any marketing campaigns that utilize customers' CPNI for a minimum of one year
3. Employees have been trained on when they are, and are not, authorized to use or disclose CPNI
    - Disciplinary process has been defined and is in place for violations and/or breaches of CPNI
4. Carrier authentication requirements have been met
    - All customer during a customer-initiated telephone call are authenticated as being an authorized account contact before discussing CPNI (non-call detail or call detail) without utilizing readily available biographical or account information as defined by the FCC
    - Call detail is only released to customers during customer-initiated telephone contact if a password is provided. If the requesting customer does not provide a password, only the following FCC approved methods are permitted for the release of the requested call detail:
        - Sending the requested detail to the address of record (only a physical or email address associated with that particular account that has been in our company files for at least 30 days)
        - Calling the customer back at the telephone of record (only disclosing if the customer was authenticated as being an authorized account contact)
        - Having customer come in to Company's office and provide a valid government issued photo ID
5. Notice to customer of account change as customers are notified immediately when a customer creates or changes one of the following:
    - password
    - customer response to a back-up means of authentication for lost or forgotten passwords
    - online account
    - address of record
6. Notice of unauthorized disclosure of CPNI, a notification process is in place in order to notify both law enforcement and customer(s) in the event of a CPNI breach within the timeline specified by the FCC
7. Opt-out method for approval of CPNI use for marketing campaigns is utilized
    - Customers are notified bi-annually of their rights for the use of their CPNI in marketing campaigns
    - New customers are notified of the opt-out procedure as a part of the customer sign-up process
    - Billing system displays customer's opting status
    - Compliance officer retains CPNI notifications and opting records for at least two years
8. Additional protection measures are taken above and beyond the current FCC CPNI rules
    - Company takes reasonable measures to discover and protect against activity that is indicative of pretexting
    - Company maintains security of all CPNI, including but not limited to:
        - Documents containing CPNI are shredded
        - Computer terminals are locked when employee is not at the station

CPNI STATEMENT

The operating procedures of Melrose Telephone Company, Mainstreet Communications, LLC and Wisper Wireless Solutions, LLC are designed to ensure compliance with the CPNI Rules applicable to them. Such procedures are as follows:

CPNI Use:

(1) We use, disclose or permit access to CPNI for marketing purposed utilizing our system which is updated to provide CPNI field with which to record the customers' response to the CPNI notice. We have also updated our software for the new CPNI rules that were effective December 8, 2007.

(2) We use, disclose to affiliates only, or permit access to CPNI to protect our rights and property and our Customers from fraudulent, abusive or unlawful use of, or subscription to, our services according to the new CPNI requirements. Additional security was added to comply with the CPNI rules effective December 8, 2007

(3) We limit the access to CPNI to provide or market service offerings among the categories of service-local and interexchange- to which Customer already subscribes. When we provide different categories of service, and a Customer subscribes to more than one service category, we share the Customer's CPNI with the affiliate that provides service to the Customer. If a Customer subscribes to only one service category, we do not share the customer CPNI with an affiliate without the Customer's approval.

(4) We use, disclose or permit access to CPNI derived from our provision of local exchange or interexchange service for the provision of CPE and call answering, voice mail or messaging, fax & store and forward and protocol conversion, without Customer approval.

(5) Without Customer approval, we do not use, disclose or permit access to CPNI to provide or market service offerings within a category of service to which the Customer does not already subscribe, except that we use, disclose or permit access to CPNI to: (a) provide inside wire maintenance and repair services; and market, when we provide local service and services formerly know as adjunct-to-basic services such as, but not limited to, speed calling, call tracing, call blocking, call return, repeat dialing, call waiting, caller ID, and call forwarding.

(6) We have updated our system of customer records to require authentication and pass code protection as required by the new rules effective December 8, 2007 and have notified our customers of these changes. We also require government issued ID when doing in store visits.

(7) We are prepared to notify Law Enforcement with in seven days after reasonable determination of any breach and shall electronically notify of United States Secret Service (USSS) and Federal Bureau of Investigation (FBI) through a central report facility which is http://www.fcc.gov/eb/cpni. We shall notify our customer of the breach after

the seven days in which the USSS & FBI have been notified unless requested by law enforcement not to notify the customer.

CPNI Approvals:

(1) When a customer calls in information on their account depending on what is required they are first authenticated. If they wants call detail etc, they then need a pass code. If coming into office must show government issued ID to obtain information for call detail they will need the pass code. We only mail customer bills or information to the customers billing address on record. When changes to the account are made notification letter is sent to the customer will follow.

CPNI Notice Requirements:

(1) We notify and inform each Customer of his or her right to restrict the use or disclosure of an access to, CPNI along with a solicitation of approval, and we maintain records of that notification, whether oral or written, for at least 1 year. We mailed notification to all customers by the end of December 2007 of the changes of the new CPNI rules. We inform all new customers prior to installation and will every 2 years send out CPNI OPT OUT notice and OPT IN notice as needed for marketing.

CPNI Safeguards:

(1) We have implemented a system by which the status of a Customer's CPNI approval can be clearly established prior to the use of the CPNI. We have clearly marked our customer records requiring authentication and pass code requirements.
(2) We have trained our personnel as to when they are, and are not authorized to use CPNI, and what is required of the customer to do to get account information.We have a Company expressed disciplinary process in place to deal with employee failures.
(3) We maintain a record of our own and our affiliates' sales and marketing campaigns that use CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign. We retain these records for 1 year.
(4) We have established a corporate officer who acts as agent for the Company and will sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the Company has established operating procedures adequate to ensure compliance with applicable CPNI rules. We will provide a Statement accompanying the Certificate that explains our operating procedures an demonstrates compliance with the CPNI rules.

(5) We are prepared to notify Law Enforcement with in seven days after reasonable determination of any breach and shall electronically notify of United States Secret Service (USSS) and Federal Bureau of Investigation (FBI) through a central report facility which is http://www.fcc.gov/eb/cpni. We shall notify our customer of the breach after the seven days in which the USSS & FBI have been notified unless requested by law enforcement not to notify the customer.